

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-102471

(43)Date of publication of application : 13.04.1999

(51)Int.Cl.

G07F 7/08

G06K 17/00

G09C 1/00

(21)Application number : 09-262489

(71)Applicant : NTT DATA CORP

(22)Date of filing : 26.09.1997

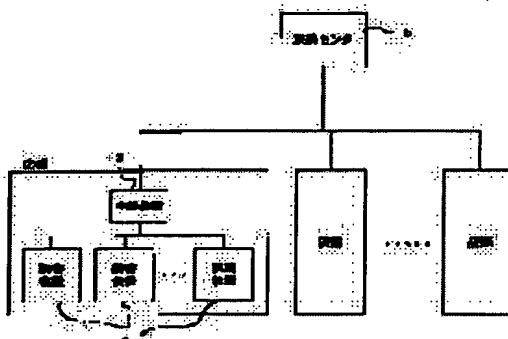
(72)Inventor : KUROI TOSHIO  
KAMATA TAKAYUKI

(54) PREPAID CARD SYSTEM, CERTIFICATION SYSTEM, READER, MANAGEMENT DEVICE, AND DEVICE CERTIFICATION METHOD

(57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a prepaid card system which can simultaneously transmit certification data to the device to be certified from a certification device, certifies them at a high speed, combines the ciphering of entire certification data and the ciphering of a part of data and discriminates the cause of the certification error of the device of the certification object.

**SOLUTION:** A relay device 3 designates a global address and simultaneously transmits all certification data to all readers 1. The respective readers 1 receiving certification data cipher a part of certification data with an individual password key, cipher the entire certification data with a common password and return them to the relay device 3. The relay device 3 decodes certification data returned from the readers 1 for certifying them commonly in the system and compares it with certification data. The relay device 3 compares a part of data certified by the readers 1 with the individual password in certification data returned from the readers 1, with the password with a block which is the object of password data for certification for individually certifying the devices.



## LEGAL STATUS

[Date of request for examination] 02.03.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-102471

(43) 公開日 平成11年(1999) 4月13日

(51) Int. Cl. <sup>9</sup>	識別記号	F I	
G 0 7 F 7/08		G 0 7 F 7/08	J
G 0 6 K 17/00		G 0 6 K 17/00	T
			L
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 F
			6 6 0 B

審査請求 未請求 請求項の数19 O L (全 16 頁) 最終頁に続く

(21) 出願番号 特願平9-262489

(22) 出願日 平成9年(1997) 9月26日

(71) 出願人 000102728

株式会社エヌ・ティ・ティ・データ  
東京都江東区豊洲三丁目3番3号

(72) 発明者 黒井 俊夫

東京都江東区豊洲三丁目3番3号 エヌ・  
ティ・ティ・データ通信株式会社内

(72) 発明者 鎌田 隆之

東京都江東区豊洲三丁目3番3号 エヌ・  
ティ・ティ・データ通信株式会社内

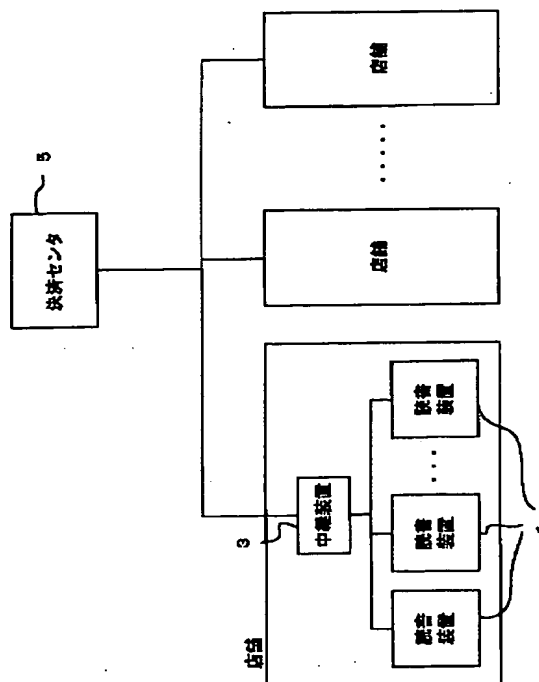
(74) 代理人 弁理士 木村 満

(54) 【発明の名称】 プリペイドカードシステム、認証システム、読書装置、管理装置及び装置認証方法

(57) 【要約】

【課題】 認証装置から認証対象装置に認証データを一齐に送信して高速に認証し、且つ、認証データ全体の暗号化と一部分のデータの暗号化とを組み合わせ、認証対象装置の認証ミスの原因を判別するプリペイドカードシステムを提供する。

【解決手段】 中継装置3は、グローバルアドレスを指定して認証データを全ての読書装置1に一齐に送信する。認証データを受信した各読書装置1は、認証データの一部分を個別暗号鍵k<sub>ei</sub>で暗号化し、さらに共通暗号鍵k<sub>f</sub>で認証データ全体を暗号化し、中継装置3に返送する。中継装置3は、読書装置1から返送された認証データを、システムで共通に認証するため、共通暗号鍵k<sub>f</sub>で復号化して、検証データと比較する。次に、中継装置3は、装置を個別に認証するため、読書装置1から返送された認証データのうち読書装置1が個別暗号鍵k<sub>ei</sub>で暗号化した一部分と検証用暗号データの対象となるブロックとを比較する。



**【特許請求の範囲】**

【請求項 1】金額情報を有するプリペイドカードを処理するための複数の読書装置と、複数の前記読書装置を管理する中継装置と、各店舗の前記中継装置と通信により接続された決済センタと、を備えるプリペイドカードシステムにおいて、

前記読書装置は、前記中継装置から送信されて来た認証データを暗号化して前記中継装置に返送し、

前記中継装置は、複数の前記読書装置に認証データを一齐に送信し、返送された各認証データから各前記読書装置を認証し、前記認証データから前記読書装置を認証できない場合に、認証できない読書装置を特定する情報と共に異常情報を前記決済センタに送信し、

前記決済センタは、前記中継装置から送信された異常情報から異常な読書装置を特定する、

ことを特徴とするプリペイドカードシステム。

【請求項 2】前記読書装置は、前記中継装置から送信されて来た認証データの一部を暗号化して前記中継装置に返送し、

前記中継装置は、返送された、一部が暗号化された認証データから各前記読書装置を認証する、

ことを特徴とする請求項 1 に記載のプリペイドカードシステム。

【請求項 3】前記読書装置は、前記中継装置から送信されて来た認証データの一部をその読書装置に固有の個別暗号化方式で暗号化し、さらに、一部が暗号化された認証データを、複数の読書装置に共通の共通暗号化方式で暗号化して前記中継装置に返送し、

前記中継装置は、返送されて来た認証データが前記共通暗号化方式で暗号化され、且つ、その一部が前記個別暗号化方式で暗号化されているか否かを判別することにより、各前記読書装置を認証する、

ことを特徴とする請求項 1 に記載のプリペイドカードシステム。

【請求項 4】前記中継装置は、検証データを前記複数の読書装置に共通の第 1 の共通暗号化方式で暗号化して認証データを生成して各読書装置に送信し、

前記読書装置は、前記中継装置から送信されて来た認証データを前記第 1 の共通暗号化方式に従って復号化した後、その一部をその読書装置に固有の個別暗号化方式で暗号化し、さらに、一部が暗号化された認証データを、前記複数の読書装置に共通の第 2 の共通暗号化方式で暗号化して前記中継装置に返送し、

前記中継装置は、返送されて来た認証データが前記第 1 及び第 2 の共通暗号化方式で適切に処理されているか否か、及び、その一部が前記個別暗号化方式で適切に暗号化されているか否かを判別することにより、各前記読書装置を認証する、

ことを特徴とする請求項 1 に記載のプリペイドカードシステム。

【請求項 5】前記中継装置には  $n$  ( $n$  は 2 以上の自然数) 台の前記読書装置が接続され、

前記認証データは  $n$  個のデータブロックを含み、

前記  $n$  台の読書装置のうち、第  $i$  ( $i$  は  $n$  以下の自然数) の読書装置は、前記中継装置から送信されて来た認証データのうちの、第  $i$  のデータブロックのデータを自己に割り当てられた個別暗号化方式で暗号化して前記中継装置に返送し、

前記中継装置は、前記第  $i$  の読書装置から返送されて来た認証データの第  $i$  のデータブロックのデータが、各読書装置に送信した認証データの第  $i$  のデータブロックに実質的に一致するか否かを判別することにより、各前記読書装置を認証する、

ことを特徴とする請求項 1 に記載のプリペイドカードシステム。

【請求項 6】前記中継装置には  $n$  ( $n$  は 2 以上の自然数) 台の前記読書装置が接続され、

前記  $n$  台の読書装置のうち、第  $i$  ( $i$  は  $n$  以下の自然数) の読書装置は、前記中継装置から受信した認証データの第  $i$  のブロックのデータを自己に割り当てられた個別暗号鍵で暗号化し、さらに、前記第  $i$  のブロックのデータが暗号化された認証データを前記共通暗号鍵で暗号化して前記中継装置に返送し、

前記中継装置は、前記第  $i$  の読書装置から返送されて来た認証データの第  $i$  のブロック以外の領域が前記共通暗号鍵により処理されているか否かを判別することと、前記第  $i$  のブロックが前記個別暗号鍵により処理されているか否かを判別することにより、各前記読書装置を認証する、

ことを特徴とする請求項 1 に記載のプリペイドカードシステム。

【請求項 7】前記中継装置には  $n$  ( $n$  は 2 以上の自然数) 台の前記読書装置が接続され、

前記中継装置は、 $n$  個のデータブロックを含む検証データを第 1 の共通暗号鍵で暗号化して認証データを生成し、

前記  $n$  台の読書装置のうち、第  $i$  ( $i$  は  $n$  以下の自然数) の読書装置は、前記中継装置から受信した認証データを前記第 1 の共通暗号鍵で復号し、復号した認証データの第  $i$  のブロックのデータを自己に割り当てられた個別暗号鍵で暗号化し、さらに、前記第  $i$  のブロックのデータが暗号化された認証データを第 2 の共通暗号鍵で暗号化して前記中継装置に返送し、

前記中継装置は、前記第  $i$  の読書装置から返送されて来た認証データの第  $i$  のブロック以外の領域が前記第 2 の共通暗号鍵により処理されているか否かを判別することと、前記第  $i$  のブロックが前記個別暗号鍵により処理されているか否かを判別することにより、各前記読書装置を認証する、

ことを特徴とする請求項 1 に記載のプリペイドカードシステム。

ステム。

【請求項 8】前記中継装置は、  
前記第  $i$  の読書装置から返送されて来た認証データの第  $i$  のブロック以外の領域が前記第 2 の共通暗号鍵により処理されているか否かを判別することにより、前記第  $i$  の読書装置がこのプリペイドカードシステムに使用可能な装置であるか否かを判別し、  
前記第  $i$  のブロックが前記個別暗号鍵により処理されているか否かを判別することにより、前記読書装置の設定のエラーの有無を判別する、  
ことを特徴とする請求項 7 に記載のプリペイドカードシステム。

【請求項 9】 $n$  台の被認証装置と、前記  $n$  台の被認証装置を管理する認証装置と、を備えるシステムにおいて、  
前記認証装置は、 $n$  個のデータブロックを含む認証データを、前記  $n$  台の被認証装置に送信し、  
前記  $n$  台の被認証装置のうち、第  $i$  ( $i$  は  $n$  以下の自然数) の被認証装置は、前記認証装置から送信されて来た認証データの第  $i$  のブロックのデータを個別の暗号鍵  $k_{ei}$  で暗号化して前記認証装置に返送し、  
前記認証装置は、前記第  $i$  の被認証装置から返送されて来た認証データの第  $i$  のブロックのデータが期待値に実質的に一致するか否かを判別することにより、各前記被認証装置を認証する、  
ことを特徴とする認証システム。

【請求項 10】前記第  $i$  ( $i$  は  $n$  以下の自然数) の被認証装置は、前記認証装置から送信されて来た認証データの第  $i$  のブロックのデータを個別の暗号鍵  $k_{ei}$  で暗号化し、前記第  $i$  のブロックのデータが暗号化された認証データを前記複数の被認証装置に共通の暗号鍵  $k_f$  で暗号化して前記認証装置に返送し、  
前記認証装置は、前記第  $i$  の被認証装置から返送されて来た認証データの第  $i$  のブロック以外のブロックのデータが期待値に実質的に一致するか否かを判別すること、及び、前記第  $i$  の被認証装置から返送されて来た認証データの第  $i$  のブロックのデータが期待値に実質的に一致するか否かを判別することにより、各前記被認証装置を認証する、  
ことを特徴とする請求項 9 に記載の認証システム。

【請求項 11】プリペイドカードを処理するための読書装置であって、  
認証データを受信する手段と、前記受信手段で受信した認証データを暗号鍵  $k_{f1}$  で復号化する復号化手段と、  
前記復号化手段により復号化された認証データ中の所定の一部のデータを暗号鍵  $k_{ei}$  で暗号化し、さらに、一部が暗号化された認証データを暗号鍵  $k_{f2}$  で暗号化して出力する手段と、  
を備えることを特徴とする読書装置。

【請求項 12】前記暗号鍵  $k_{f1}$  と前記暗号鍵  $k_{f2}$  は、実質的に等しい、

ことを特徴とする請求項 11 に記載の読書装置。

【請求項 13】プリペイドカードを処理するための読書装置を認証して管理する上位装置であって、  
認証データを複数の読書装置に一斉に送信する送信手段と、  
各読書装置から送信されて来た認証データを受信する受信手段と、  
前記受信手段で受信した認証データに基づいて各読書装置を認証する認証手段と、  
を備えることを特徴とする管理装置。

【請求項 14】前記認証手段は、前記受信手段で受信した認証データが期待値に実質的に一致するか否かを判別することにより、認証を行う、ことを特徴とする請求項 13 に記載の管理装置。

【請求項 15】前記送信手段は、検証データを複数の読書装置に共通の暗号鍵  $k_f$  で暗号化して認証データを生成して前記複数の読書装置に送信し、  
前記認証手段は、前記受信手段で受信した認証データを前記暗号鍵  $k_f$  で復号化し、復号化したデータが実質的に期待値に一致するか否かに基づいて各読書装置を認証する、  
ことを特徴とする請求項 14 に記載の管理装置。

【請求項 16】前記認証手段は、前記受信手段で受信した認証データを前記暗号鍵  $k_f$  で復号化し、前記暗号鍵  $k_f$  で復号化した認証データの、各読書装置に割り付けられた一部が前記検証データに実質的に一致するか否かに基づいて各読書装置を認証する、  
ことを特徴とする請求項 15 に記載の管理装置。

【請求項 17】プリペイドカードから得た金額情報を取り扱う装置を認証する方法であって、  
認証データを一度に複数の認証相手装置に送信する一斉送信ステップと、  
前記一斉送信ステップで送信された認証データを受信し、受信した認証データを暗号鍵で暗号化し、暗号化した認証データを返送する認証データ更新ステップと、  
前記認証データ更新ステップから返送された認証データを受信する受信ステップと、  
前記受信ステップで受信した認証データと認証相手装置を認証することのできる検証データとを比較して認証相手装置を認証する認証ステップと、  
を備えることを特徴とする装置認証方法。

【請求項 18】同一の認証データを複数の相手装置に一斉送信し、  
各相手装置が、受信した認証データのうちの対応する一部をその装置に割り当てられた暗号鍵で暗号化し、一部が暗号化された認証データを返送し、  
返送された認証データを受信し、  
受信した認証データと前記検証データとを比較して認証相手装置を認証する、  
ことを特徴とする装置認証方法。

【請求項 19】同一の認証データを複数の認証相手装置に送信する際に、該複数の認証相手装置に共通の暗号化方式で暗号化して一斉送信し、各相手装置が、受信した認証データを復号化した後、復号化したデータのうちの対応する一部をその装置に割り当てられた暗号鍵で暗号化し、一部が暗号化された認証データを共通の暗号化方式で暗号化して返送し、返送された認証データを受信し、受信した認証データと前記検証データとを比較して認証相手装置を認証する、ことを特徴とする装置認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、通信による装置の認証を高速化することのできるプリペイドカードシステム、認証システム、読書装置及び装置認証方法に関する。

【0002】

【従来の技術】従来のプリペイドカードシステムにおいて、プリペイドカードに記憶されている金額情報を使用するための読書装置は、使用された金額情報等をセンタ等の上位装置に送信する。上位装置は、このような金額情報等が、売上金となる重要なデータであるため、セキュリティ上、正当なデータであり、しかも正しい相手からのデータであることを確認する必要がある。

【0003】上位装置は、読書装置が正しい相手であることを確認するために、通信により装置の認証を行う。通信による装置の認証を、例えば、秘密鍵暗号方式の場合について説明すると、まず、認証側の装置となる上位装置は、平文のデータ A を相手装置となる読書装置に送信する。読書装置は、受信したデータ A を、記憶している暗号鍵  $k_e$  を使用して暗号化し、データ A' とする。読書装置は、暗号化したデータ A' を上位装置に返送する。上位装置は、読書装置から返送されたデータ A' と、読書装置に送信した平文のデータ A を自ら記憶している暗号鍵  $k_e$  を使用して暗号化しておいたデータ A' とを比較する。上位装置は、互いの暗号鍵  $k_e$  を使用して暗号化された 2 つのデータ A' が一致すると判別した場合に、読書装置が正しい相手であることを認証する。また、上位装置が、多数の読書装置を認証する場合には、認証相手である読書装置毎に異なる暗号鍵を認証に使用して、データ改竄や偽造装置からの偽造データの発生に対する安全性を高めている。

【0004】

【発明が解決しようとする課題】しかし、大規模なプリペイドカードシステムともなると、読書装置が多数設置されているため、全ての読書装置を個別に認証すると、装置認証による負荷が大きくなる。このため、一般的に、公開鍵暗号方式よりも比較的处理を高速に行える秘密鍵暗号方式を認証に用いるなどの対策をしても、認証

に必要なデータの送受信に時間がかかるため、認証を高速化することが困難であった。

【0005】また、読書装置ごとに異なる暗号鍵を認証に使用する場合では、暗号鍵の配付の誤りや読書装置の設置の誤り等、設定上の誤りが発生する割合が高くなる。従って、読書装置の認証できなかった場合でも、データ改竄や偽造装置が原因と断定する前に、設定の確認が必要となり、迅速な対処をすることが困難となっていた。

【0006】本発明は、上記実状に鑑みてなされたもので、通信による読書装置の認証を高速化することができるプリペイドカードシステム、認証システム、読書装置、管理装置及び装置認証方法を提供することを目的とする。また、本発明は、設定上の誤りを原因とする読書装置の認証不能を適切に判別することのできるプリペイドカードシステム、認証システム、読書装置、管理装置及び装置認証方法を提供することを目的とする。

【0007】

【課題を解決するための手段】上記目的を達成するため、この発明の第 1 の観点に係るプリペイドカードシステムは、金額情報を有するプリペイドカードを処理するための複数の読書装置と、複数の前記読書装置を管理する中継装置と、各店舗の前記中継装置と通信により接続された決済センタと、を備えるプリペイドカードシステムにおいて、前記読書装置は、前記中継装置から送信されて来た認証データを暗号化して前記中継装置に返送し、前記中継装置は、複数の前記読書装置に認証データを一斉に送信し、返送された各認証データから各前記読書装置を認証し、前記認証データから前記読書装置を認証できない場合に、認証できない読書装置を特定する情報と共に異常情報を前記決済センタに送信し、前記決済センタは、前記中継装置から送信された異常情報から異常な読書装置を特定する、ことを特徴とする。

【0008】このような構成によれば、中継装置から読書装置へ認証データの送信を一斉にすることで認証を高速化することができる。また、中継装置は、読書装置を認証できない場合に、異常情報を中継装置の上位装置である決済センタに送信する。決済センタは、受信した異常情報から該当する読書装置を特定することができる。従って、最上位装置である決済センタが最下位装置である読書装置の認証異常を把握することができる。

【0009】読書装置は、中継装置から送信されて来た認証データの一部を暗号化して中継装置に返送し、中継装置は、返送された、一部が暗号化された認証データから各読書装置を認証してもよい。この構成によれば、中継装置は、一部が暗号化された認証データから、読書装置を認証する。従って、読書装置は、認証データの一部のみを暗号化すればよく、結果として、システム全体の認証を高速化することができる。

【0010】読書装置は、中継装置から送信されて来た

認証データの一部をその読書装置に固有の個別暗号化方式で暗号化し、さらに、認証データ全部を、各読書装置に共通の共通暗号化方式で暗号化して中継装置に返送し、中継装置は、返送されて来た認証データが共通暗号化方式で暗号化され、且つ、その一部が個別暗号化方式で暗号化されているか否かを判別することにより、各読書装置を認証してもよい。

【0011】この構成によれば、中継装置は、共通暗号化方式による暗号化が不適切なために認証データを認証できない場合には、その装置自体に何らかの異常（偽物装置である可能性を含めて）があると推測できる。また、共通暗号化方式による暗号化は適切に行われているが、個別暗号化方式による暗号化が不適切なために認証データを認証できない場合には、読書装置の設定のミスなどが原因であると推測できる。従って、異常の原因の推測も可能である。

【0012】また、中継装置は、検証データを複数の読書装置に共通の第1の共通暗号化方式で暗号化して認証データを生成して各読書装置に送信し、読書装置は、中継装置から送信されて来た認証データを第1の共通暗号化方式に従って復号化した後、その一部をその読書装置に固有の個別暗号化方式で暗号化し、さらに、一部が暗号化された認証データを、複数の読書装置に共通の第2の共通暗号化方式で暗号化して中継装置に返送し、中継装置は、返送されて来た認証データが第1及び第2の共通暗号化方式で適切に処理されているか否か、及び、その一部が個別暗号化方式で適切に暗号化されているか否かを判別することにより、各前記読書装置を認証してもよい。

【0013】この構成によれば、認証データが第1及び第2の共通暗号化方式で適切に処理されているか否かを判別することにより、読書装置の異常を推測することができる。また、認証データが第1及び第2の共通暗号化方式で適切に処理されているが、個別暗号化方式で適切に処理されていない場合には、読書装置の設定や配置のミスであることが推測できる。従って、異常の原因の推測も可能である。

【0014】例えば、中継装置には、 $n$  ( $n$ は2以上の自然数) 台の読書装置が接続され、認証データは  $n$  個のデータブロックを含み、 $n$  台の読書装置のうち、第  $i$

( $i$ は  $n$ 以下の自然数) の読書装置は、中継装置から送信されて来た認証データのうちの、第  $i$  のデータブロックのデータを自己に割り当てられた個別暗号化方式で暗号化して中継装置に返送し、中継装置は、第  $i$  の読書装置から返送されて来た認証データの第  $i$  のデータブロックのデータが、各読書装置に送信した認証データの第  $i$  のデータブロックに実質的に一致するか否かを判別することにより、各前記読書装置を認証してもよい。

【0015】この構成によれば、複数の読書装置に同一の認証データを送信しながら、読書装置を個別に認証す

ることができる。

【0016】第  $i$  の読書装置は、中継装置から受信した認証データの第  $i$  のブロックのデータを自己に割り当てられた個別暗号鍵で暗号化し、さらに、認証データ全体を共通暗号鍵で暗号化して中継装置に返送し、中継装置は、第  $i$  の読書装置から返送されて来た認証データの第  $i$  のブロック以外の領域が共通暗号鍵により処理されているか否かを判別することと、第  $i$  のブロックが個別暗号鍵により処理されているか否かを判別することにより、各前記読書装置を認証してもよい。

【0017】この構成によれば、中継装置は、読書装置が共通暗号鍵と個別暗号鍵とを適切に使用できるか否かにより認証することができる。しかも、共通暗号鍵を適切に使用できるか否かにより、このプリペイドカードシステムで使用できる読書装置であるか否かを推測することができ、個別暗号鍵を適切に使用できるか否かにより、読書装置の設定などのミスの有無等を推測できる。即ち、異常の原因を推測することも可能である。

【0018】また、中継装置が、認証データを共通暗号鍵で暗号化してから、各読書装置に送信し、各読書装置が受信した認証データを復号してから、上述の処理を行うようにしてもよい。

【0019】中継装置は、第  $i$  の読書装置から返送されて来た認証データの第  $i$  のブロック以外の領域が共通暗号鍵により処理されているか否かを判別することにより、第  $i$  の読書装置がこのプリペイドカードシステムに使用可能な装置であるか否かを判別し、第  $i$  のブロックが個別暗号鍵により処理されているか否かを判別することにより、前記読書装置の設定のエラーの有無を判別することができる。

【0020】中継装置は、第  $i$  の読書装置から返送された認証データを、第  $i$  のブロック以外の領域が共通暗号鍵により処理されているか否かと、第  $i$  のブロックが個別暗号鍵により処理されているか否かと、から第  $i$  の読書装置を認証する。従って、中継装置は、第  $i$  の読書装置を認証できない場合に、第  $i$  のブロック以外の領域と第  $i$  のブロックから認証できない原因を判別することができる。

【0021】また、この発明の第2の観点に係る認証システムは、 $n$  台の被認証装置と、前記  $n$  台の被認証装置を管理する認証装置と、を備えるシステムにおいて、前記認証装置は、 $n$  個のデータブロックを含む認証データを、前記  $n$  台の被認証装置に送信し、前記  $n$  台の被認証装置のうち、第  $i$  ( $i$ は  $n$ 以下の自然数) の被認証装置は、前記認証装置から送信されて来た認証データの第  $i$  のブロックのデータを個別の暗号鍵  $k_{ei}$  で暗号化して前記認証装置に返送し、前記認証装置は、前記第  $i$  の被認証装置から返送されて来た認証データの第  $i$  のブロックのデータが期待値に実質的に一致するか否かを判別することにより、各読書装置を認証する。

【0022】この構成によれば、認証装置から一度に複数の被認証装置に同一の認証データを送って、各被認証装置の認証処理が可能となる。

【0023】第*i*の被認証装置は、認証装置から送信されて来た認証データの第*i*のブロックのデータを個別の暗号鍵*k<sub>e</sub><sub>i</sub>*で暗号化し、第*i*のブロックのデータが暗号化された認証データを複数の被認証装置に共通の暗号鍵*k<sub>f</sub>*で暗号化して認証装置に返送し、認証装置は、第*i*の被認証装置から返送されて来た認証データの第*i*のブロック以外のブロックのデータが期待値に実質的に一致するか否かと、第*i*の被認証装置から返送されて来た認証データの第*i*のブロックのデータが期待値に実質的に一致するか否かとを判断することにより、各被認証装置を認証してもよい。

【0024】この構成によれば、共通暗号鍵*k<sub>f</sub>*による認証ができない場合には、被認証装置がシステム内で使用できない装置であることが推測できる。一方、個別暗号鍵*k<sub>e</sub><sub>f</sub>*による認証ができない場合には、被認証装置の配置や設定のミスであることが推測できる。

【0025】また、この発明の第3の観点に係る読書装置は、プリペイドカードを処理するための読書装置であって、認証データを受信する手段と、前記受信手段で受信した認証データを暗号鍵*k<sub>f</sub><sub>1</sub>*で復号化する復号化手段と、前記復号化手段により復号化された認証データの所定の一部のデータを暗号鍵*k<sub>e</sub><sub>i</sub>*で暗号化し、さらに、認証データ全体を暗号鍵*k<sub>f</sub><sub>2</sub>*で暗号化して出力する手段と、を備えることを特徴とする。

【0026】このような構成によれば、読書装置は、認証データの一部を暗号鍵*k<sub>e</sub><sub>i</sub>*で暗号化し、さらに、認証データ全体を暗号鍵*k<sub>f</sub><sub>2</sub>*で暗号化して出力する。従って、読書装置からこのような認証データを返送された上位装置等は、読書装置を認証できない場合に、暗号鍵*k<sub>e</sub><sub>i</sub>*で暗号化された認証データの一部と暗号鍵*k<sub>f</sub><sub>2</sub>*で暗号化された認証データとから認証できない原因を判断することができる。

【0027】暗号鍵*k<sub>f</sub><sub>1</sub>*と暗号鍵*k<sub>f</sub><sub>2</sub>*は、実質的に等しくてもよい。

【0028】また、この発明の第4の観点に係る管理装置は、プリペイドカードを処理するための読書装置を認証して管理する上位装置であって、認証データを複数の読書装置に一齐に送信する送信手段と、各読書装置から送信されて来た認証データを受信する受信手段と、前記受信手段で受信した認証データに基づいて各読書装置を認証する認証手段と、を備えることを特徴とする。

【0029】このような構成によれば、管理装置は、読書装置に認証データを一齐に送信し、各読書装置から返送された認証データを検証することにより、各読書装置の認証をすることができる。従って、中継装置から読書装置へ認証データの送信を一齐にすることで認証を高速化することができる。

【0030】認証手段は、受信手段で受信した認証データが期待値に実質的に一致するか否かを判断することにより、認証を行ってもよい。

【0031】送信手段は、検証データを複数の読書装置に共通の暗号鍵*k<sub>f</sub>*で暗号化して認証データを生成して複数の読書装置に送信し、認証手段は、受信手段で受信した認証データを暗号鍵*k<sub>f</sub>*で復号化し、復号化したデータが実質的に期待値に一致するか否かに基づいて認証してもよい。

【0032】認証手段は、受信手段で受信した認証データを暗号鍵*k<sub>f</sub>*で復号化し、暗号鍵*k<sub>f</sub>*で復号化した認証データの、各読書装置に割り付けられた一部が前記検証データに実質的に一致するか否かに基づいて認証してもよい。

【0033】また、この発明の第4の観点に係る装置認証方法は、プリペイドカードから得た金額情報を取り扱う装置を認証する方法であって、認証データを一度に複数の認証相手装置に送信する一斉送信ステップと、前記一斉送信ステップで送信された認証データを受信し、受信した認証データを暗号鍵で暗号化し、暗号化した認証データを返送する認証データ更新ステップと、前記認証データ更新ステップから返送された認証データを受信する受信ステップと、前記受信ステップが受信した認証データと認証相手装置を認証することのできる検証データとを比較して認証相手装置を認証する認証ステップと、を備える、ことを特徴とする。

【0034】このような方法によれば、認証相手装置に認証データを一齐に送信し、各認証相手装置から返送された認証データを検証することにより、各認証相手装置の認証をすることができる。従って、認証相手装置へ認証データの送信を一齐にすることで認証を高速化することができる。

【0035】同一の認証データを複数の相手装置に一齐送信し、各相手装置が、受信した認証データのうちの対応する一部をその装置に割り当てられた暗号鍵で暗号化し、一部が暗号化された認証データを返送し、返送された認証データを受信し、受信した認証データと検証データとを比較して認証相手装置を認証してもよい。

【0036】一部が暗号化された認証データから認証データを暗号化した認証相手装置を認証する。従って、各認証相手装置の暗号化処理が速くなり、全体の認証を高速化することができる。

【0037】同一の認証データを複数の認証相手装置に送信する際に、複数の認証相手装置に共通の暗号化方式で暗号化して一斉送信し、各相手装置が、受信した認証データを復号化した後、復号化したデータのうちの対応する一部をその装置に割り当てられた暗号鍵で暗号化し、一部が暗号化された認証データを共通の暗号化方式で暗号化して返送し、返送された認証データを受信し、受信した認証データと検証データとを比較して認証相手

装置を認証してもよい。

【0038】認証相手装置が割り当てられた暗号鍵で一部を暗号化した認証データを受信し、受信した認証データと検証データを比較して認証相手装置を認証する。従って、認証相手装置を認証できない場合に、一部を暗号化された認証データから認証できない原因を判別することができる。

【0039】

【発明の実施の形態】本発明の実施の形態にかかるプリペイドカードシステムについて以下図面を参照して説明する。このプリペイドカードシステムは、図1に示すように、各店舗に設置された読書装置1及び中継装置3と、決済センタ5と、を備える。

【0040】読書装置1は、例えば、商品（サービス）の購入、貸出、提供等の対価の支払の場面において、プリペイドカードが記憶する金額情報を使用するための装置である。読書装置1は、各店舗に配置され、図2に示すように、カード読書部11と、記憶部13と、制御部15と、通信制御部17と、を備える。

【0041】カード読書部11は、装着されたプリペイドカードに記憶されているデータの読取り／書込みを行う。

【0042】記憶部13は、読書装置1で使用（消費）された決済金額情報を記憶する。また、記憶部13は、上位装置となる中継装置3から認証のために認証データが送信された際に、認証データの更新処理に使用する共通暗号鍵kfと個別暗号鍵ke（例えば、DES方式の秘密鍵等）を記憶する。共通暗号鍵kfは、全ての読書装置1に共通の暗号鍵である。また、個別暗号鍵keは、読書装置1ごとに異なる暗号鍵である。さらに、記憶部13は、自らを識別する装置ID（装置識別コード）を記憶する。

【0043】制御部15は、プリペイドカードの使用要求に応答し、使用金額に応じて、カード読書部11に装着されているプリペイドカードの金額（残高）情報を更新すると共に、記憶部13に記憶している決済金額情報に使用金額を加算する。また、制御部15は、上位装置となる中継装置3から認証のために認証データが送信された際に、通信制御部17を介して認証データを受信し、記憶部13に記憶された共通暗号鍵kfと個別暗号鍵keを使用して受信した認証データを更新し、通信制御部17を介して中継装置3に返送する。

【0044】通信制御部17は、中継装置3との通信を制御する。

【0045】図1に示す中継装置3は、店舗内に設置されている各読書装置1から決済金額情報を受信し、それらを集約（集計等）して、所定のタイミングで決済センタ5に送信する。また、中継装置3は、各読書装置1を認証するため、所定のタイミングで、店舗内の全ての読書装置1に共通に設定されているグローバルアドレスを

指定して、全読書装置1に認証データを一斉に送信する。

【0046】中継装置3は、図3に示すように、記憶部21と、制御部23と、通信制御部25と、を備える。

【0047】記憶部21は、通信制御部25を介して店舗内の各読書装置1から受信した決済金額情報を記憶する。また、記憶部21は、複数の読書装置1に共通な共通暗号鍵kfと各読書装置1に固有の個別暗号鍵ke（ke1、ke2、・・・、ken；nは読書装置1の数）を記憶する。共通暗号鍵kfは、全ての読書装置1の記憶部13に記憶されている共通暗号鍵kfと同一の暗号鍵である。また、複数の個別暗号鍵ke（ke1、ke2、・・・、ken）は、各読書装置1の記憶部13に記憶されている個別暗号鍵keにそれぞれ1対1に対応する（同一である）。

【0048】また、記憶部21は、各読書装置1を認証するために使用する図4（a）に示す検証データと、図4（b）に示す検証用暗号データと、図4（c）に示す認証データと、を記憶する。

【0049】検証データは、図4（a）に示す様に、n（nは読書装置の数）個のデータブロックを有する平文データから構成されている。検証用暗号データは、図4（b）に示す様に、図4（a）の検証データをデータブロックごとに対応する個別暗号鍵ke（ke1、ke2、・・・、ken）を使用して暗号化したデータ（データ1'～データn'）から構成される。認証データは、図4（c）に示す様に、図4（a）の検証データ全体を共通暗号鍵kfを使用して暗号化したデータ（データ1''～データn''）から構成される。さらに、記憶部21は、自らを識別する装置IDを記憶する。

【0050】制御部23は、通信制御部25を介して店舗内の各読書装置1から受信した決済金額情報を集計し、店舗単位の決済金額の合計を示す決済合計額情報を生成する。また、制御部23は、所定のタイミングで店舗内の各読書装置1が、正しい下位装置であるか否かを判別するため、図4（c）の認証データをグローバルアドレスを指定し、通信制御部25を介して全読書装置1に一斉に送信する。さらに、制御部23は、各読書装置1で更新され、返送された認証データを使用して送信元の読書装置1を認証する認証処理を行う。

【0051】通信制御部25は、読書装置1及び決済センタ5との間の通信を制御する。

【0052】図1に示す決済センタ5は、各店舗の中継装置3から決済合計額情報を受信し、それらを集約（集計等）する。決済センタ5は、図5に示すように、記憶部31と、制御部33と、通信制御部35と、を備える。

【0053】記憶部31は、通信制御部35を介して各中継装置3から受信した決済合計額情報を記憶する。また、記憶部31は、各中継装置3を識別するID情報



と、各中継装置 3 の下位装置となる各読書装置 1 を識別する ID 情報とを記憶する。

【0054】制御部 33 は、通信制御部 35 を介して各中継装置 3 から受信した決済合計額情報を集計する。また、制御部 33 は、中継装置 3 が下位装置である読書装置 1 を認証できない場合に送信する異常情報を通信制御部 35 を介して受信し、受信した異常情報から該当する読書装置 1 を特定すると共に異常原因を特定する異常処理を行う。

【0055】通信制御部 35 は、中継装置 3 との通信を制御する。

【0056】次に、本システムの動作について、中継装置 3 が読書装置 1 に対して行う認証処理の流れに沿って説明する。

【0057】まず、中継装置 3 が店舗内の読書装置 1 に対して行う認証処理を、各読書装置 1 がその際行う認証データ更新処理と合わせて、図 6 及び図 7 のフローチャートを参照して説明する。中継装置 3 は、図示せぬタイマ装置から得られる所定のタイミング或いは決済センタ 5 からの要請に基づいて、図 6 に示す下位装置認証処理を開始する。まず、中継装置 3 は、通信制御部 25 を介して、図 4 (c) に示す認証データと認証処理の実行を指示する指示コマンドとを、読書装置 1 のグローバルアドレス（共通アドレス）を指定して各読書装置 1 に一斉に送信する（ステップ S1）。

【0058】認証データを受信した各読書装置 1 は、図 7 に示す認証データ更新処理を開始する。まず、制御部 15 は、通信制御部 17 を介して受信した認証データ（図 4 (c)）全体を、共通暗号鍵  $k_f$  を使用して復号化し、図 8 (a) に示す平文の認証データ（図 4 (a) に示す検証データに等しい）を生成する（ステップ S11）。

【0059】次に、各読書装置 1 の制御部 15 は、復号化した認証データのうちの、自己に割り付けられたデータブロックのデータを記憶部 13 に記憶された個別暗号鍵  $k_{ei}$  を使用して暗号化する（ステップ S12）。例えば、論理的に第  $i$  の読書装置 1 は、個別暗号鍵  $k_{ei}$  を使用して、復号化された認証データ中の第  $i$  のデータブロックを、図 8 (b) に示すように暗号化する。なお、 $i$  は、記憶部 13 に記憶された装置 ID から特定される装置の論理的番号であり、 $1 \sim n$  の整数である。

【0060】次に、制御部 15 は、図 8 (b) に示すように第  $i$  のデータブロックだけが更新された認証データ全体を、図 8 (c) に示すように、共通暗号鍵  $k_f$  を使用して暗号化する（ステップ S13）。なお、個別暗号鍵  $k_{ei}$  で暗号化され、更に共通暗号鍵  $k_f$  で暗号化されたデータ  $i$  をデータ  $i''$  と表す。

【0061】制御部 15 は、図 8 (d) に示すように、暗号化した更新済認証データに装置 ID 等を含むヘッダ情報を付加して、通信制御部 17 を介して中継装置 3 に

送信する（ステップ S14）。

【0062】中継装置 3 は、図 6 に示すステップ S2 で、読書装置 1 で更新された認証データ（図 9 (a)）を通信制御部 25 を介して受信する。中継装置 3 は、受信したヘッダ情報と認証データとを分離し、分離した認証データを記憶部 21 に記憶された共通暗号鍵  $k_f$  を使用して復号化する（ステップ S3）。これにより、図 9 (b) に示すように、第  $i$  のデータブロックだけが暗号鍵  $k_{ei}$  で更新（暗号化）された検証データが生成される。

【0063】次に、中継装置 3 は、ヘッダ情報に含まれている装置 ID から、更新されているデータブロックを判別し、図 9 (c) 及び (d) に示すように、更新ブロック（データブロック  $i$ ）と他の未更新データブロック（データブロック  $1 \sim i-1, i+1 \sim n$ ）とに分離する（ステップ S4）。

【0064】中継装置 3 は、記憶部 21 に記憶されている図 4 (a) に示す検証データから、図 9 (b) に示す未更新データブロックを抽出する。中継装置 3 は、検証データから抽出したデータと、図 9 (d) に示す受信した未更新データブロックとが一致するか否かを判別する（ステップ S5）。

【0065】検証データから抽出したデータと受信した未更新データブロックとが一致しない場合は、認証対象の読書装置 1 が共通暗号鍵  $k_f$  を適切に使用して認証処理ができない異常な装置の場合である。従って、中継装置 3 は、通信制御部 25 を介して、装置異常を示す異常コードと読書装置 1 を特定する装置 ID と、中継装置 3 を識別する装置 ID とからなる異常情報を決済センタ 5 に送信する（ステップ S7）。

【0066】一方、検証データから抽出したデータと受信した未更新データブロックとが一致すると判別された場合、中継装置 3 は、予め記憶部 21 に記憶された図 4 (b) に示す検証用暗号データから、受信した装置 ID で特定されるデータブロックと同一のデータブロック（データブロック  $i$ ）を抽出する。中継装置 3 は、この抽出したデータブロックと、図 9 (c) に示す更新データブロック（データブロック  $i$ ）とが一致するか否かを判別する（ステップ S6）。

【0067】抽出したデータブロックと更新データブロックとが一致しない場合は、読書装置 1 自体は共通暗号鍵  $k_f$  でデータを処理できる装置、即ち、このシステムで利用できる装置であるが、装置 ID や暗号鍵  $k_{ei}$  の設定が不適切なものと推定される。そこで、中継装置 3 は、設定異常を示す識別コードと、読書装置 1 を特定する装置 ID と、中継装置 3 を識別する装置 ID とからなる異常情報を決済センタ 5 に送信する（ステップ S8）。

【0068】一方、ステップ S6 で抽出したデータブロック（データブロック  $i$ ）と更新データブロック（デー

タブロック i) とが一致すると判別された場合は、認証データを返送した読書装置 1 が、暗号鍵 k f と k e i を適切に使用できるものであることから、中継装置 3 との間で個別に認証されたこととなり、中継装置 3 は、必要に応じて、任意の処理を開始する。

【0069】次に、決済センタ 5 が中継装置 3 から異常情報を受信した場合の異常装置特定処理を、図 10 のフローチャートを参照して説明する。

【0070】中継装置 3 から異常情報を受信した決済センタ 5 は、図 10 に示す異常処理を開始する。まず、制御部 33 は、通信制御部 17 を介して受信した異常情報から中継装置 3 を識別する装置 ID と読書装置 1 を識別する装置 ID とを抽出する。制御部 33 は、抽出した 2 つの装置 ID から該当する読書装置 1 及びその店舗を特定する (ステップ S 21)。

【0071】次に、制御部 33 は、受信した異常情報から異常識別コードを抽出し、抽出した異常識別コードが装置異常を示すか設定異常を示すかを判別する (ステップ S 22)。

【0072】制御部 33 は、抽出した識別コードが装置異常 (即ち、共通暗号鍵 k f による認証エラー) を示す場合は、図示せぬ表示装置にステップ S 21 において特定した読書装置 1 及びその店舗を示す装置情報と、装置異常を示す異常メッセージとを表示し、管理者に通知する (ステップ S 23)。装置異常が通知された管理者は、偽物装置による不当な売り上げを防止するため、例えば、該当する読書装置 1 の上位装置となる中継装置 3 から受信した決済情報の集計を停止する等の処置を取る。また、該当する読書装置 1 の回収等を保守作業者に連絡する。

【0073】一方、制御部 33 は、ステップ S 22 において、識別コードが装置異常を指示しているものではないと判別した場合に、抽出した識別コードが設定異常を示しているか否かを判別する (ステップ S 24)。

【0074】制御部 33 は、抽出した識別コードが設定異常を示している場合に、図示せぬ表示装置に異常が検出された読書装置 1 及びその店舗を示す装置情報と、設定異常を示すメッセージとを表示し、管理者に通知する (ステップ S 25)。設定異常は、読書装置 1 自体は、このプリペイドカードシステムで使用可能な正当な装置であるが、何らかの原因で、個別暗号鍵 k e i が誤って設定されたり、装置の配置が誤っているなどの原因で発生すると推測される。そこで、読書装置 1 の設定異常を通知された管理者は、例えば、該当する読書装置 1 の再設定を保守作業者に連絡する。

【0075】一方、制御部 33 は、ステップ S 24 において、識別コードが設定異常を指示しているものではないと判別した場合に、予め設定された他の理由による不正データを受信したものと判別する。制御部 33 は、図示せぬ表示装置にステップ S 21 において特定した読書

装置 1 及びその店舗を示す装置情報と、不正データ受信を示す異常メッセージとを表示し、管理者に通知する (ステップ S 26)。

【0076】以上説明したように、この実施の形態では、中継装置 3 は、認証データを複数の読書装置 1 に一斉に送信し、各読書装置 1 から返送されて来た認証データを認証に使用する。このため、通信による読書装置 1 の認証を高速化することができる。また、二重に暗号化された認証データを認証に使用することにより、共通暗号鍵 k f で認証されなかった読書装置 1 を偽物装置の可能性が高いと推測し、個別暗号鍵 k e i で認証できなかった読書装置 1 を誤って設定された装置であると推測することができる等、認証エラーの原因も推測することができる。

【0077】上記の実施の形態では、中継装置 3 が各読書装置 1 に対してだけ認証処理を行ったが、さらに決済センタ 5 が各中継装置 3 に対して認証処理を行ってもよい。決済センタ 5 が各中継装置 3 に対する認証処理を行うことで、全体としてのセキュリティを向上させることができる。

【0078】中継装置 3 が、読書装置 1 から受信した認証データが正当なものであるか否かを判別する手法は任意である。

【0079】例えば、上記実施の形態では、第 i の読書装置の共通暗号鍵 k f を用いた認証のために、データブロック i 以外のデータブロックが検証データに一致しているか否かを判別している。しかし、読書装置の設置ミスの場合には、データブロック i 以外のデータブロックが更新されて返送される場合があり、検証データと受信したデータブロックが完全には一致しないこともあり得る。このため、受信した認証データのうちのデータブロック i 以外の殆どのブロック (例えば、全体のデータブロックの 80%) が検証ブロックに一致する場合には、両データが一致すると判別し、装置異常は存在しないと判断してもよい。

【0080】例えば、中継センタ 3 は、第 i の読書装置 1 から受信した認証データを共通暗号鍵 k f で復号化し、復号化された認証データのうちの第 1 ~ 第 i-1 及び第 i+1 ~ 第 n のデータブロックが検証データ (期待値) と一致するか否かを判別することにより装置異常を検出し、第 i のデータブロックを個別暗号鍵 k e i で復号化し、復号化された第 i のデータブロックと検証データの第 i のデータブロック (期待値) が一致するか否かを判別することにより個別的な認証を行ってもよい。

【0081】また、受信データの期待値を予め用意しておき、受信した認証データを復号することなく、認証を行ってもよい。例えば、中継センタ 3 は、第 i の読書装置 1 から受信した認証データの期待値を予め用意しておき、受信した認証データの第 1 ~ 第 i-1 及び第 i+1 ~ 第 n のデータブロックと期待値の対応部分が一致するか否か

を判別することにより、装置異常の有無を検出し、受信した認証データの第 i のデータブロックと期待値の対応部分とを比較することにより、設定異常の有無を検証してもよい。この場合、受信データを復号化することなく、認証を行うことができ、認証を高速化できる。

【0082】その他、この発明は、認証側の装置において、受信した認証対象のデータが共通暗号鍵及び個別暗号鍵により適切に処理（暗号化、復号化）されているかを判別することができるならば、判別手法は任意に選択可能である。

【0083】なお、認証処理を実行するタイミングは、任意である。例えば、中継装置 3 の図示せぬ入力部から認証指示が入力されたタイミングで認証処理を開始してもよい。この構成により、読書装置 1 に使用する暗号鍵の変更作業や読書装置 1 の設置作業の完了時に、認証処理を実施し、作業の確認をすることができる。

【0084】また、中継装置 3 が検証データを暗号化するために使用する共通暗号鍵と各読書装置 1 が更新済みの認証データを暗号化するために使用する共通暗号鍵は異なってもよい。また、共通暗号鍵を使用する方法に限定されず、複数の読書装置 1 に共通ならば、他の暗号方式を使用してもよい。

【0085】さらに、各読書装置は、個別暗号鍵を互いに異ならせるだけでなく、暗号化方式自体を異ならせてもよい。

【0086】中継装置 3 および読書装置 1 を構成するネットワーク形状は、任意である。例えば、リング型のネットワーク形状としてもよい。

【0087】以上の実施の形態では、中継装置 3 が認証データのグローバルアドレスを指定し各読書装置 1 に一斉に送信しているが、通信プロトコル等の制約から 1 電文の最大長が決まっている場合は、複数回に分けて送信してもよい。例えば、HDL C 手順の場合に、認証データの 1 データブロックを 8 バイトとすると、中継装置 3 は、1 フレームで約 32 台の読書装置 1 に認証データを送信することができる。このとき、読書装置 1 が 32 台より多い場合には、中継装置 3 は、認証データを複数のフレームに分けて送信する。

【0088】また、この発明は、プリペイドカードシステムに適用する場合に限定されず、ある管理装置が複数

の管理対象装置を認証する場合に広く適用可能である。

【0089】

【発明の効果】以上説明したように、本発明によれば、認証装置から認証対象装置に認証データを一斉に送信することにより、認証処理を高速化することができる。また、認証データ全体の暗号化と一部分のデータの暗号化とを組み合わせ使用することにより、認証対象装置の認証ミスの原因を判別することができる。

【図面の簡単な説明】

【図 1】本発明の実施の形態に係るプリペイドカードシステムの構成を示す図である。

【図 2】読書装置 1 の構成を示す図である。

【図 3】中継装置 3 の構成を示す図である。

【図 4】検証データ、検証用暗号データ及び認証データを示す図である。

【図 5】決済センタ 5 の構成を示す図である。

【図 6】上位装置が行う認証処理のフローチャートである。

【図 7】下位装置が行う認証データ更新処理のフローチャートである。

【図 8】下位装置で更新（暗号化）される認証データを示す図である。

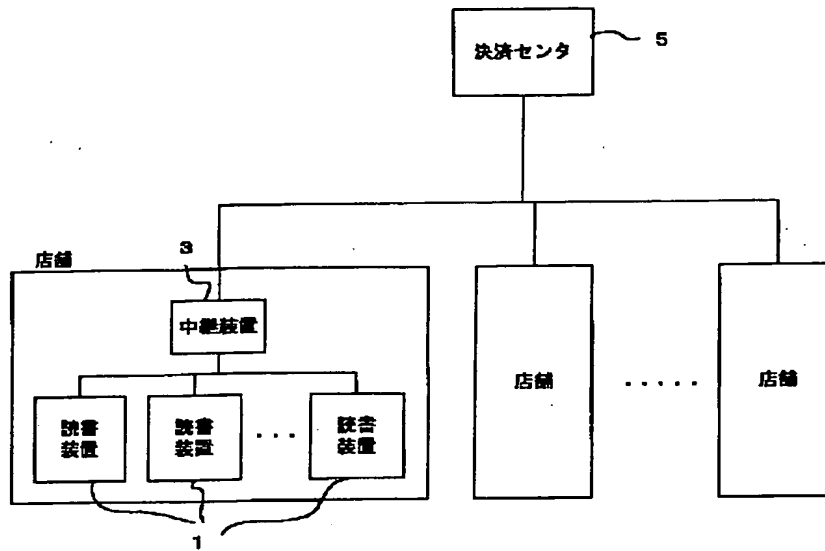
【図 9】上位装置で認証（データ分離等）される認証データを示す図である。

【図 10】上位装置が行う異常装置特定処理のフローチャートである。

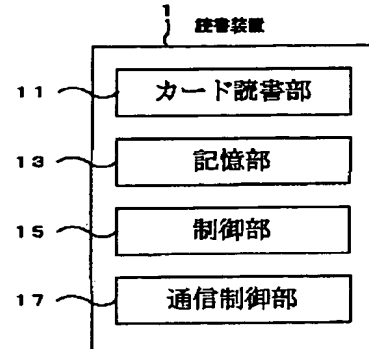
【符号の説明】

1	読書装置
3	中継装置
5	決済センタ
11	カード記録部
13	記憶部
15	制御部
17	通信制御部
21	記憶部
23	制御部
25	通信制御部
31	記憶部
33	制御部
35	通信制御部

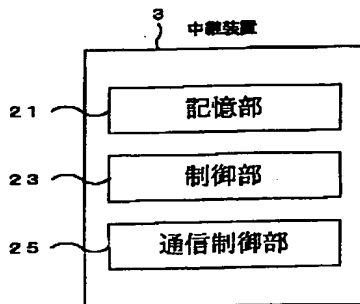
【図1】



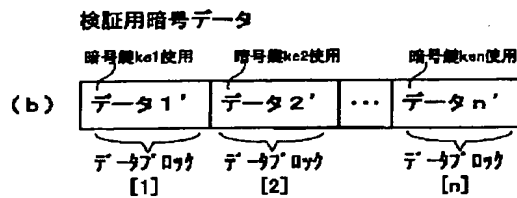
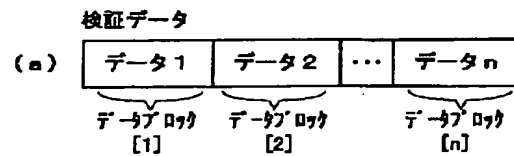
【図2】



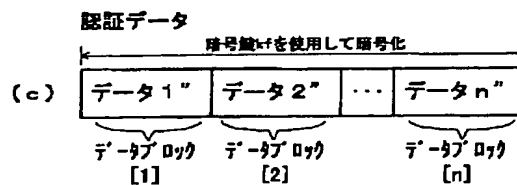
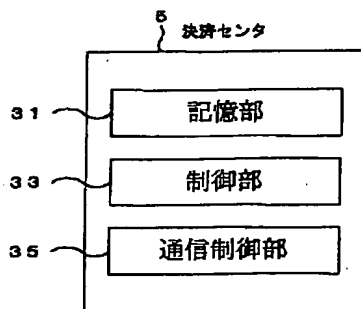
【図3】



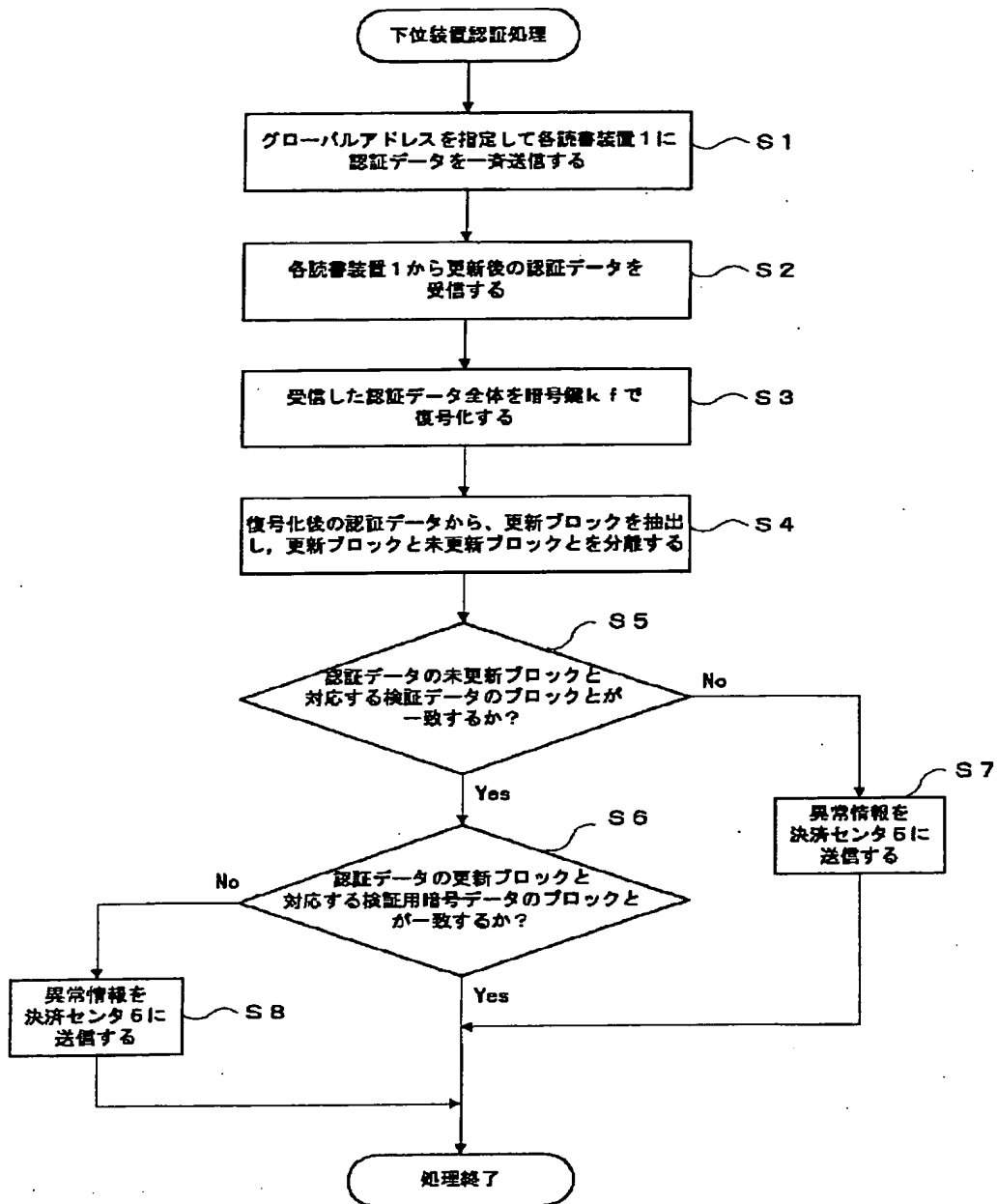
【図4】



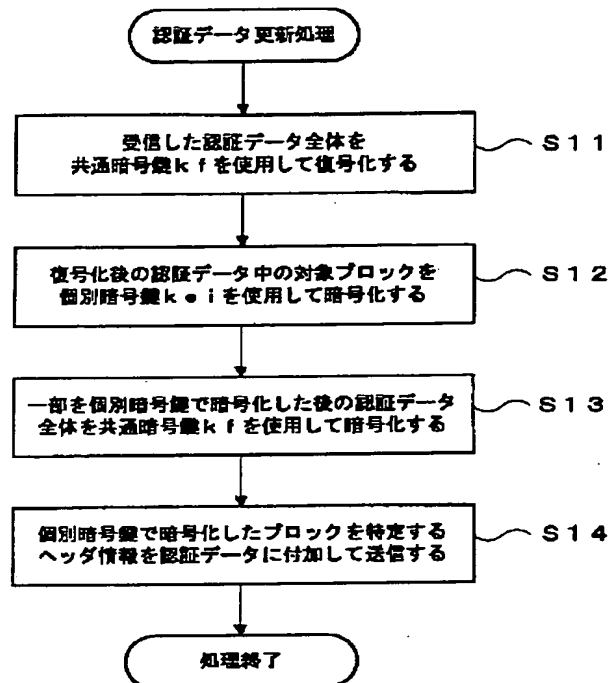
【図5】



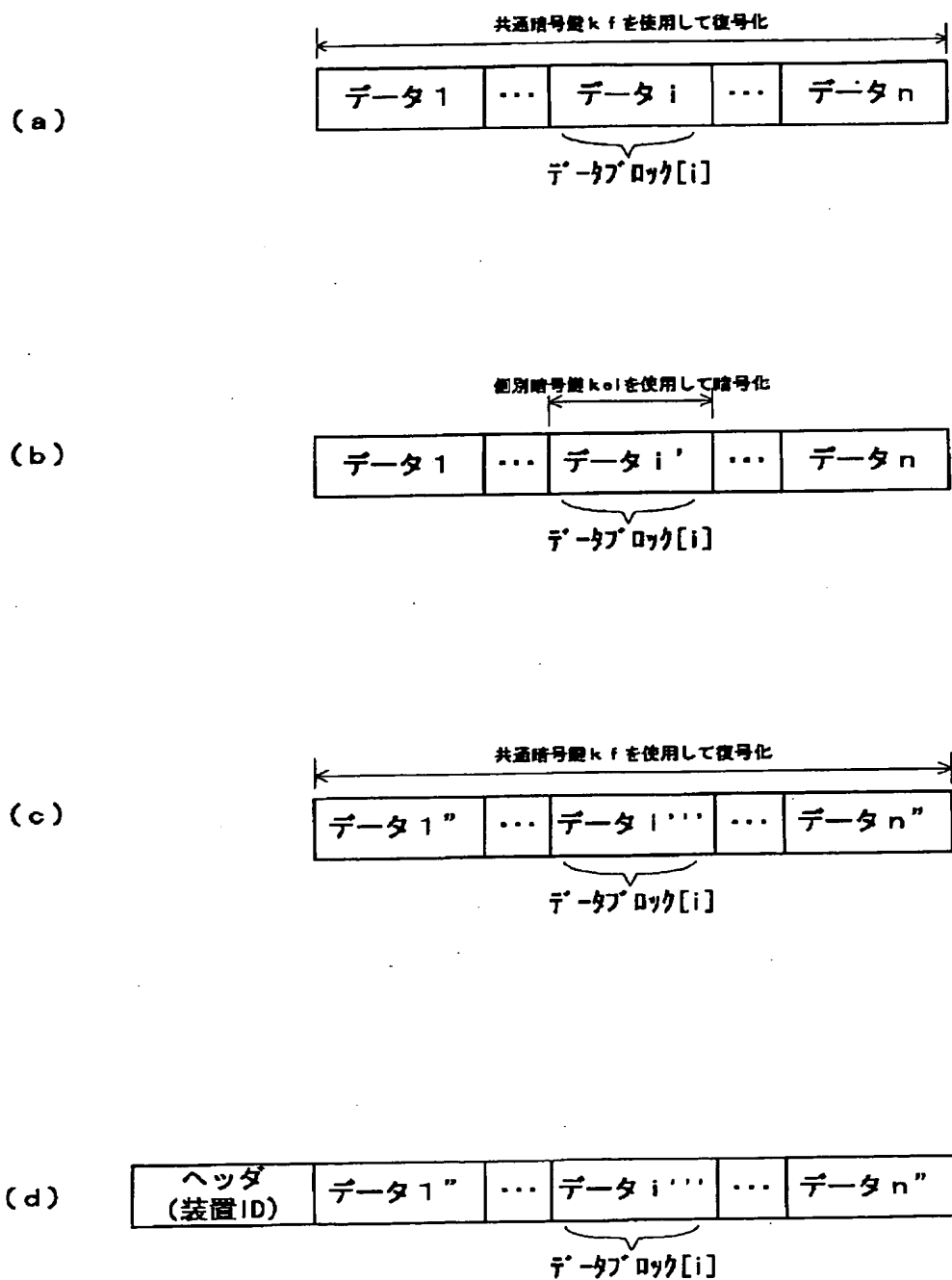
【図 6】



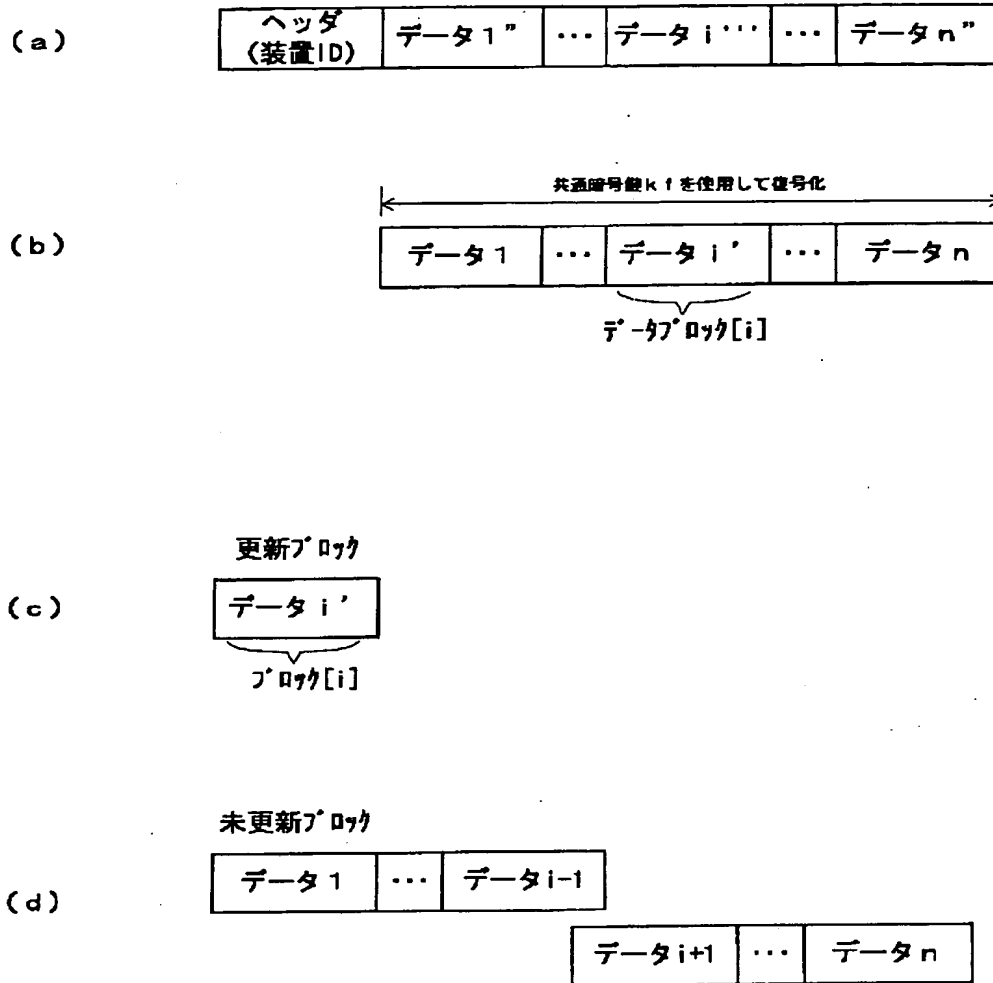
【図 7】



【図8】

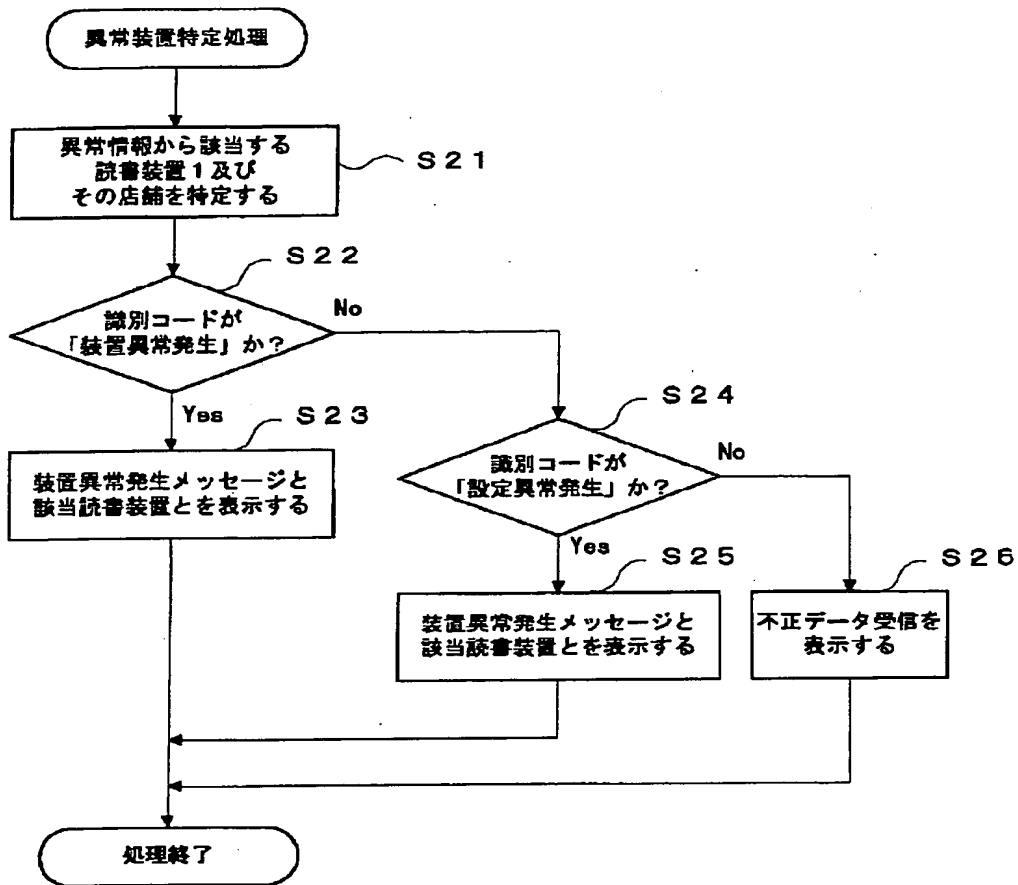


【図 9】





【図 10】



フロントページの続き

(51) Int. Cl. 6

識別記号

F I  
G O 7 F 7/08

L